BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellants	:	Alain Durand et al.
Serial No.	:	10/532,193
Filed	:	April 21, 2005
Title	:	**SIMPLIFIED METHOD FOR RENEWING SYMMETRICAL KEYS IN A DIGITAL NETWORK**
Examiner	:	Michael R. Vaughan
Art Unit	:	2431

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

In response to the Final Office Action dated April 7, 2010, and further to the Notice of Appeal filed on July 7, 2010, Appellants hereby submit an Appeal Brief in accordance with 37 C.F.R. §41.37 for the above-referenced application.

I. Real Party in Interest

The real party in interest is THOMSON Licensing S.A., 46 Quai A. Le Gallo, F-92100 Boulogne-Billancourt, France.

II. Related Appeals and Interferences

There are no prior or pending appeals, interferences, or judicial proceedings known to Appellants, the Appellants' legal representative, or assignee which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. Status of Claims

Claims 1-4 are pending in this application, and are rejected. The rejection of claims 1-4 is being appealed.

IV. Status of Amendments

No amendment subsequent to the final rejection of April 7, 2010 has been filed.

V. Summary of Claimed Subject Matter

Independent claim 1 defines a method for encrypting data in a communication network comprising a device of a first type (see, for example, page 2, lines 28-29) containing:

- a first symmetric key for encrypting the data to be sent to a device of a second type connected to the network, wherein said second type of device is a different device type from said device of a first type (see, for example, page 2, lines 30-31); and

- and an encrypted first symmetric key which is generated from the encryption of said first symmetric key with a second symmetric network key known only by at least one device of a second type connected to said network (see, for example, page 2, lines 32-34);

the method comprising the steps for the device of a first type of:

(a) generating a random number (see, for example, page 2, lines 35-36);

(b) computing a new symmetric key as a function of the first symmetric key and said random number (see, for example, page 2, lines 36-37);

(c) encrypting the data to be transmitted with the new symmetric key (see, for example, page 2, line 37 to page 3, line 1); and

(d) transmitting to a device of a second type, via said network (see, for example, page 3, lines 1-2):

- the data encrypted with the new symmetric key (see, for example, page 3, line 3);
- the random number (see, for example, page 3, line 4); and
- said encrypted first symmetric key (see, for example, page 3, lines 5-6).

VI. Ground of Rejection to be Reviewed on Appeal

The rejection of claims 1-4 under 35 U.S.C. §103(a) based on the proposed combination of Menezes et al. "Handbook of Applied Cryptography, PASSAGE." Handbook of Applied Cryptography, CRC Press Series on Discrete Mathematics and its Applications, Boca Raton, FL, CRC Press, US, 1997, pages 497-553 (hereinafter, "Menezes") and U.S. Patent Publication No. 2005/0025091 by Patel et al. (hereinafter, "Patel") is presented for review in this appeal.

VII. Argument

The rejection of claims 1-4 under 35 U.S.C. §103(a) based on the proposed combination of Menezes and Patel should be reversed for at least the following reasons.

Appellants first note that the sole independent claim at issue in this appeal, claim 1, recites the following:

> "Method for encrypting data in a communication network comprising a device of a first type containing:
>
> - a first symmetric key for encrypting the data to be sent to a device of a second type connected to the network, wherein said second type of device is a different device type from said device of a first type; and

- and an encrypted first symmetric key which is generated from the encryption of said first symmetric key with a second symmetric network key known only by at least one device of a second type connected to said network;

the method comprising the steps for the device of a first type of:

(a) generating a random number;

(b) computing a new symmetric key as a function of the first symmetric key and said random number;

(c) encrypting the data to be transmitted with the new symmetric key; and

(d) transmitting to a device of a second type, via said network:

- the data encrypted with the new symmetric key;
- the random number; and
- said encrypted first symmetric key."

Appellants respectfully submit that neither Menezes nor Patel, whether taken individually or in combination, discloses or suggests each and every one of the features defined by claim 1.

In the final Office Action of April 7, 2010, the Examiner alleges that most of the features of claim 1 are taught by the Needham-Schroeder (hereinafter, "N-S") key exchange protocol described on page 503 of Menezes. For example, the Examiner alleges that Menezes' random value N_B corresponds to the "random number" of claim 1.

Appellants respectfully disagree. In particular, according to Menezes, A (i.e., the alleged "device of a first type" of claim 1) does not generate this random value N_B. Moreover, A does not send random value N_B to B (i.e., the alleged "device of a second type" of claim 1). Rather, Menezes clearly teaches that A sends N_B-1 to B. Accordingly, Menezes fails to disclose or suggest, *inter alia*, the features of "the method comprising the steps for the device of a first type of: (a) generating a random number… and (d) transmitting to a device of a second type, via said network: … the random number", as recited by claim 1. Patel is unable to remedy these deficiencies of Menezes. Therefore, for this reason alone, Appellants respectfully submit that the instant rejection should be reversed.

Also in the final Office Action of April 7, 2010, the Examiner ostensibly alleges that the features of "an encrypted first symmetric key which is generated from the encryption of said first symmetric key with a second symmetric network key known only by at least one device of a second type connected to said network" of claim 1 are disclosed by Menezes when A sends E_{kBT}(k,A) to B. Also in the argument, the Examiner states that Menezes may be combined with Patel, in which case A generates the new symmetric key, encrypts it with the second symmetric key, and sends the encrypted key to B.

In response, Appellants question how the aforementioned functions are possible if A doesn't have the second symmetric key, as claimed (i.e., "a second symmetric network key known only by at least one device of a second type")? Accordingly, the Examiner's proposed combination would appear to be counter-intuitive to those skilled in the art.

In addition, the key used to encrypt the new session key can be said to be a session key in itself. As such, Appellants submit that one skilled in the art would have absolutely no motivation to go to the trouble of generating a second session key (note that this is not a new session key, but a second, parallel session key) when A and B already share one. Accordingly, Appellants submit that the proposed combination appears to be undesirable to those skilled in the art and thus, the result of impermissible hindsight reconstruction. Here, Appellants note that the mere fact that a prior art device could (in hindsight) be modified to produce a claimed invention is not a basis for an obviousness rejection unless the prior art suggests the desirability of such a modification. See, for example, *In re Laskowski*, 871 F.2d 115, 10 USPQ2d 1397 (Fed. Cir. 1989) ("Although the Commissioner suggests that [the structure in the primary prior art reference] could readily be modified to the form the [claimed] structure, '[t]he mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification.'") and *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984).

Appellants further note that it is not proper to try to read *first* a classical N-S protocol and *then* the N-S-Patel combination onto claim 1, as, for example, the first device does not have access to the encrypted first symmetric key until part of the classical N-S protocol has been performed.

Accordingly, for at least the foregoing reasons, Appellants submit that claims 1-4 are patentable over the proposed combination of Menezes and Patel under 35 U.S.C. §103(a), and respectfully request that the Board reverse the rejection of claims 1-4.

The fee for this Appeal Brief is being charged Deposit Account 07-0832 using EFS-Web. Please charge this Deposit Account for any additional fees owed in connection with this Appeal Brief.

Respectfully submitted,
Alain Durand et al.

By: /Joel M. Fogelson/
Joel M. Fogelson
Attorney for Appellants
Reg. No. 43,613
Phone (609) 734-6809

Patent Operations
Thomson Licensing LLC
P. O. Box 5312
Princeton, New Jersey 08540

August 18, 2010

VIII. Claims Appendix

1. Method for encrypting data in a communication network comprising a device of a first type containing:

- a first symmetric key for encrypting the data to be sent to a device of a second type connected to the network, wherein said second type of device is a different device type from said device of a first type; and

- and an encrypted first symmetric key which is generated from the encryption of said first symmetric key with a second symmetric network key known only by at least one device of a second type connected to said network;

the method comprising the steps for the device of a first type of:

(a) generating a random number;

(b) computing a new symmetric key as a function of the first symmetric key and said random number;

(c) encrypting the data to be transmitted with the new symmetric key; and

(d) transmitting to a device of a second type, via said network:

- the data encrypted with the new symmetric key;
- the random number; and
- said encrypted first symmetric key.

2. Method according to claim 1, wherein the function used to compute the new symmetric key is a one-way derivation function.

3. Method according to claim 2, wherein the function is a hash function.

4. Method according to claim 1, also comprising the steps for the device of a second type that receives data transmitted at step (d) of :

(e) decrypting, with the second symmetric network key the encrypted first symmetric key as to produce the first symmetric key;

(f) determining, based on the first symmetric key obtained at step (e) and on said random number, the new symmetric key; and

(g) decrypting the data received with the new symmetric key.

IX. Evidence Appendix

None.

X. Related Proceedings Appendix

None.